图书情报工作
第 64 卷 第 7 期 2020 年 4 月

移动健康应用程序的隐私政策评价及实证研究*

■ 马骋宇 刘乾坤
首都医科大学公共卫生学院卫生管理与政策学系 北京 100069

摘 要：[目的/意义] 分析主流中文移动健康应用程序的隐私政策现状，提出完善我国移动健康应用隐私保护机制的建议。[方法/过程] 通过 3 轮筛选选取 104 款移动健康应用程序的隐私政策文本作为研究对象，基于内容分析法分析文本内容，再构建综合评价指标体系对隐私政策的内容进行系统评价。[结果/结论] 移动健康应用程序的隐私政策整体评价得分不高，平均得分为 44.58 分（100 分满分），隐私政策在规范性和完备性上均需完善，部分应用程序存在过度收集和滥用用户隐私数据的情况。从优化隐私政策设计，规范评价和监管机制，完善用户健康隐私信息保护的法律环境 3 个方面提出政策建议。

关键词：隐私政策 移动健康 隐私保护 监管机制
分类号：G25
DOI：10.13266/j.issn.0252－3116.2020.07.006

"互联网＋医疗健康"是依托新一代信息技术，提供以健康管理、病情咨询、挂号用药服务等各项应用为主的医疗服务新模式[1]。近年来，在健康中国和"互联网＋"战略的共同推动下，"互联网＋医疗健康"在我国呈现快速发展态势。随着智能手机的普及，移动健康应用程序（以下简称移动健康 APP）被广泛使用，用户在移动手机端披露个人健康隐私信息的机会越来越多，一方面，有利于用户获得高质量、个性化的医疗健康服务；另一方面，也带来了较高的信息安全风险。为此，2017 年 12 月国家标准化管理委员会颁布《信息安全技术 个人信息安全规范》（GB/T 35273－2017，以下简称《规范》），明确了对个人信息控制者在信息收集、保存、使用、共享、转让和披露等方面行为的规范，同时也提供了模板，为移动健康 APP 完善隐私保护政策提供依据，但目前执行效果如何尚缺乏定量评价。为此，本研究通过分析我国主流移动健康 APP 隐私政策实践现状，发现存在的问题，并提出对策建议，为完善移动健康 APP 隐私安全保护机制提供依据。

1 国内外移动健康平台的隐私政策评价研究现状

随着移动互联网日益渗透到人们的学习、工作和生活中，移动 APP 为手机用户提供各种便利服务的同时，也记录和传输了用户的大量个人信息。移动 APP 的高频使用和大量信息的交换与传播使得隐私安全问题备受关注。目前，国际上对移动 APP 的个人隐私信息保护主要存在两种模式：以欧盟为代表的立法模式和以美国为代表的企业自律模式[2]。我国则采用软件运营者自律为主、政府监管为辅的模式，即政府相关部门出台条例和规范，软件运营者自行制定隐私保护政策，对用户隐私安全保护相关的权利、义务及责任进行明示[3]。因此，隐私保护政策已成为移动 APP 隐私保护安全链上的重要一环，帮助用户了解在使用平台服务时自身哪些信息会被收集、如何收集、为何收集，如何保存和使用以及信息安全事件发生后的处置和补救措施等[4]。然而，根据 2018 年中国消费者协会对 100 款各类 APP 的调查报告结果显示，在隐私政策的可见性方面，将近 34% 的 APP 不对用户公布个人隐私保护条款，41% 未在明显位置公示隐私政策；而在自我规制的可读性方面，隐私政策内容晦涩难懂、框架不清晰，91% 的 APP 存在过度收集个人信息的现象。APP 在个人信息保存期限、信息存储地以及安全应急处置措施等方面评分仅为 1.2－1.5 分（满分 3 分）[5]。

移动健康 APP 是移动 APP 在医疗健康领域的具

* 本文系国家社会科学基金青年项目"在线医疗服务对医疗服务体系的影响效应及引导机制研究"（项目编号：16CGL066）研究成果之一。
作者简介：马骋宇（ORCID：0000－0002－2458－8422），副教授，博士，E-mail：machengyu@ccmu.edu.cn；刘乾坤（ORCID：0000－0001－8478－150X），硕士研究生。
收稿日期：2019－07－22 修回日期：2019－10－13 本文起止页码：46－55 本文责任编辑：易飞

马骋宇，刘乾坤. 移动健康应用程序的隐私政策评价及实证研究[J]. 图书情报工作,2020,64(7):46－55.

体应用,与普通移动应用相比,移动健康 APP 除了涉及用户的姓名、出生年月、性别、职业、电话号码、Email 地址等身份信息外,还可能在提供疾病预防、体检、诊断、治疗等服务过程中获取用户的健康诊疗信息[6],因此,隐私性更强,安全要求更高。近年来,移动健康 APP 的隐私保护政策应用实践及评价研究受到了国内外研究者的关注。研究者们从不同的角度对移动健康 APP 的隐私政策进行调查和分析,调查领域涉及医疗健康咨询、慢病管理、药物管理和家庭监测等,评价维度包括采集和收集、保存和维护、使用和访问、共享和转让以及咨询和反馈等多个环节,分析方法主要为内容分析法、文本分析法、比较分析等如表 1 所示:

表 1　隐私政策评价体系相关研究

著者及发表时间	APP 数量	APP 种类(领域)	评价维度	指标数量	分析方法
P. R. Croll (2011 年)[13]	3 款	健康	从信息收集者、收集类型、共享、披露、授权访问以及信任缺失的后果等 8 方面分析隐私政策	8 项指标	案例研究
M. Rowan (2014 年)[14]	20 款	医疗健康	应用权限获取和可读性测试分析	2 个维度	比较分析
B. C. Zapata 等(2014 年)[8]	24 款(Android 和 IOS)	电子健康档案	从隐私政策访问、变更通知、认证机制、数据加密、安全标准和法律规范约束、第三方是否授权 6 方面分析隐私政策质量 6 项指标	内容分析	
朱颖 (2017 年)[15]	11 类 96 款(IOS 端)	手机浏览器、新闻资讯、影音播放、社交应用、移动电商、金融理财、健康医疗、生活服务等	(1)一般情况:从隐私政策拥有、位置、规范性及动态性等分析; (2)具体内容:从信息采集内容、目的、方法、未成年人保护、用户权利等分析	2 个维度 15 项指标	内容分析
刘娇等 (2017 年)[16]	11 类 55 款	社交、电商、银行、理财、视频、游戏、新闻、旅游、健康、教育、医疗等	从隐私声明拥有、位置呈现方式、文本详细程度、敏感信息收集和使用、信息共享、未成年信息使用、数据安全技术 7 个方面分析	7 项指标	文本分析
B. Mariam 等 (2018 年)[9]	19 款(Android 7 款和 IOS 12 款)	怀孕监控	(1)从隐私政策位置、更改通知、存取管理分析隐私; (2)从数据管理、未经授权访问、访问审核、访问标准、验证和保障措施分析安全方面; (3)从标准或规定分析遵守法规方面	3 个维度 35 项指标	内容分析
A. C. Powell 等 (2018 年)[17]	70 款 Android	糖尿病和心理健康	从字数、每段句子、每句单词、每个单词字符、阅读轻松度、Gunning Fog 得分、SMOG 指数、自动可读性指数等 15 个指标来分析隐私政策复杂性	15 项指标	内容分析
L. Parker 等 (2019 年)[18]	61 款	心理健康	从隐私权政策的可访问性和可读性、数据收集使用和共享、安全和信息泄露的投诉以及 GDPR 法规对隐私政策影响 4 方面分析隐私权政策	4 个维度	内容分析
L. Rosenfeld 等(2017 年)[19]	72 款	痴呆	(1)从隐私政策是否存在、数据保护措施等分析隐私政策一般特征; (2)从信息采集、共享、出售、披露、用户是否可以删除/修改个人信息等方面分析	2 个维度 11 项指标	内容分析
J. M. Robillard 等(2019 年)[20]	(IOS 319 款和 Android 69 款)	心理健康	(1)通过在线可读性计算器计算隐私政策的可读性; (2)从隐私政策信息的性质、种类、使用、第三方共享信息性质、第三方类型、披露信息原因、安全措施等方面对隐私政策进行内容分析	2 个维度	内容分析

然而,国内外相关研究表明,移动健康 APP 的隐私政策存在可读性不强、整体得分普遍不高的问题。A. Sunyaev 等研究 600 个移动健康应用程序 APP 隐私政策质量时发现,仅有 30.5% 拥有隐私政策,且隐私政策的阅读也需要用户具有大学水平的读写能力,同时 66.1% 的隐私政策不针对应用程序自身功能[7]。B. C. Zapata 等从隐私政策访问、变更通知、认证机制、数据加密、安全标准和法律规范约束、第三方是否授权访问 6 方面分析和评估了 24 款包含患者电子病历的移动健康 APP,发现其隐私政策评分均低于 3.5 分(满分 6 分)[8]。B. Mariam 等采用涵盖隐私、安全性以及标准和法规特征的模板来评估 19 个妊娠监测移动 APP 的隐私策略(iOS 为 12 个,Android 为 7 个),发现 19 个隐私政策均未完全符合所评估模板研究的特征[9]。A. Sunyaev 等发现大多数运动健康 APP 会在缺乏用户知情同意下收集个人信息[10]。48.8% 糖尿病管理移动 APP 与第三方共享用户的个人健康信息[8]。国内关于移动健康 APP 的隐私政策评价研究主要涵盖在综合性调查中,在 2018 年一项针对 1 000 款常见 APP 的隐私政策透明度调查中发现,医疗健康类 APP 虽然透明度相对较高,但评分仅为 42.2 分(满分 100 分)[11－12]。

通过对已有研究的分析表明,国外针对移动健康的隐私政策评价研究较为丰富,国内研究较少,且大多

涵盖在综合性调查中，缺少针对移动健康 APP 特定领域的大样本隐私政策调查结论。为此，本研究通过构建隐私政策评价指标体系，对目前安卓商店中主流的移动健康 APP 的隐私政策文本质量进行评价，为进一步推动我国移动健康 APP 健康发展，提升行业自律水平，加强政府监管效果提供政策建议。

2 移动健康 APP 隐私政策的发展现状研究

2.1 研究对象

根据 2019 年 6 月的凯度移动通信消费者指数（Kantar Worldpanel ComTech）显示，中国智能手机操作系统市场中，Android（安卓）占市场份额的 79.9%，IOS 占 19.7%，其他仅占 0.4%[21]。且通过比对发现，IOS 商店中排名前 200 的移动医疗健康 APP 均开发了安卓版本。因此，本研究以安卓应用商店内的移动健康 APP 作为研究对象。按照服务内容的不同，本研究将移动健康 APP 分为移动健康、移动医疗、互联网医院移动端 3 类：①移动健康类 APP 主要包括健康管理、健身运动、慢病管理等功能，如 Keep、小米运动、咕咚、每日瑜伽等；②移动医疗类 APP 主要包括预约挂号、在线问诊功能，且主办主体为第三方平台，如平安好医生、1 号药店、微医、阿里健康等；③互联网医院移动端 APP 主要是线下实体医院的移动手机端应用，使用和开发主体均为线下的实体医院，如儿童医院挂号、中国医大一院、浙二好医生等。

本研究于 2019 年 1 月对安卓应用商店中的移动健康 APP 进行了 3 轮筛选。首先选取截至 2018 年 12 月 31 日下载量大于 1 万的 APP 共 589 款；之后将没有独立隐私政策或隐私声明的 APP 剔除，共收集有隐私政策文本的 APP 269 款；然后剔除隐私政策文本重复的 APP（存在同一公司下属多个 APP 共用一个隐私政策文本的情况），最终得出具有独立隐私政策文本的 APP 共 104 款。其中，移动健康类 42 款，移动医疗类 52 款，互联网医院类 10 款，见表 2。

2.2 主要研究内容及结论

本文采用的主要研究方法是内容分析法（content analysis）。内容分析法是一种对文献内容作客观、系统和量化描述的研究方法[22]，它通过将内容归类为预先定义的类别，从而将定性信息定量化。本研究的文献样本是经过 3 轮筛选后得到的 104 个中文移动健康 APP 的隐私政策文本。研究人员将 104 个隐私政策保存为文本文件，同时记录隐私政策的收集位置、下载量和用户评分。

表 2 抽样移动健康 APP 情况分析

项目	APP 性质	APP 数目（款）	占比（%）
类别	移动健康	42	40.38
	移动医疗	52	50.00
	互联网医院移动端	10	9.62
下载量（万次）	[1,50)	66	63.46
	[50,500)	23	22.11
	[500,1 000)	8	7.69
	[1 000,5 000)	5	4.81
	[5 000,+∞)	2	1.92
应用商店评分（分）	[0,1)	5	4.81
	[1,2)	8	7.69
	[2,3)	12	11.54
	[3,4)	25	24.04
	[4,5]	54	51.92
合计		104	100.00

然后，本文结合已有研究及《规范》要求制定分析体系。分析体系包括 27 项客观指标，大部分选项为“是”或“否”，少数指标的取值可以通过统计满足选项的个数获得。为确保分析的一致性和信度，先由 2 名研究人员分别对数据进行测度，结果显示一致性达 95% 以上，表明分析结果信度较好。

在具体指标设置上，本研究发现相关研究及《规范》对个人隐私信息的安全保护已经贯穿生产、采集、存储、加工、共享、利用和反馈各个环节，覆盖了数据的整个生命周期。因此，本研究从数据生命周期的视角，构建移动健康 APP 隐私政策评价体系的一级指标，包括隐私政策属性、个人信息的收集、存储、使用、共享、反馈共 6 个维度。在此基础上，对照《规范》要求，生成二级、三级指标。进而研究移动 APP 运营者在数据生命周期的各个环节对《规范》的理解和执行情况，发现服务供需双方个人隐私信息权力和义务的对等情况，从而分析数据生命周期在个人隐私信息保护实践中的辐射状况。基于数据生命周期构建指标体系，调查移动健康 APP 的隐私政策，可以更加清晰地了解用户的隐私保护现状，发现移动健康 APP 存在的风险环节，了解《规范》在现实中的落实情况。

2.2.1 隐私政策的长度、更新频率和设计原则

可见性和可读性是隐私政策重要的合规标准，本研究通过调查隐私文本的位置来测度其可见性，通过调查隐私政策文本的长度、要点目录、更新情况、设计原则等反映隐私政策的可读性。隐私文本长度如果过短，会在一定程度上影响隐私政策的完整性；如果过长，则会显得冗长繁杂，加之文本内容晦涩难懂，会影

响用户的阅读和理解。调查发现,被抽样 APP 的隐私文本平均长度为 4 190 个字,中位数为 2 846 个字。为方便阅读,仅 19 款 APP 为用户提供了隐私政策要点目录。从最近更新时间来看,被抽样的 104 款移动健康 APP 中,仅 22 款(占 21.15%)标注了隐私政策动态更新时间,其中 17 款更新时间在 2018 年之后。

用户一旦注册使用 APP,软件提供商就会成为用户个人健康信息的实际控制者。《规范》要求,隐私信息控制者需要遵循权责一致、目的明确、选择同意、最少够用、确保安全、主体参与、公开透明等原则。研究发现样本 APP 中有 10 款提到遵循用户选择同意原则,11 款保证会合理利用用户个人信息,一款名为"医事通"的 APP 提到会将隐私保护融入产品设计作为信息安全基本原则。

2.2.2 个人信息收集阶段

就信息收集阶段来看,用户在下载、注册移动健康 APP 过程中,平台可能会向用户收集个人身份证明信息、通信及通讯信息、个人健康生理信息、个人财产及支付信息和位置、住址信息等。隐私保护政策健全的移动健康 APP 应告知收集用户信息的种类和用途,否则将存在个人隐私信息泄露的风险。研究结果显示,104 款 APP 中有 61 款(占58.65%)告知了用户收集其个人信息的用途和方式;30 款(占 28.85%)没有说明收集个人信息的种类;70 款(占 67.31%)收集了个人的身份证明信息;39 款(占 37.50%)收集了个人健康生理信息数据,如表 3 所示:

表 3 隐私政策个人信息收集种类情况

个人信息收集种类	APP 数目(款)	占比(%)
个人身份证明数据	70	67.31
通信通讯数据	65	62.50
日志数据、Cookie 等	55	52.89
位置信息等数据	51	49.04
个人健康生理信息等数据	39	37.50
个人财产信息	31	29.81
无说明	30	28.85

注:一款抽样 APP 会采集一种或多种个人信息

Cookie 技术等自动工具是软件开发商或运营商用于追踪用户痕迹的小型数据文件,有利于收集用户特征信息,了解、分析、管理用户行为。因此,移动健康 APP 在使用 Cookie 等工具时,应对其使用目的和拒绝使用情况作详细的描述。调查结果发现,104 款 APP 中有 57 款(占 54.81%)明确表示会使用 Cookie,其中 44 款告知了用户使用 Cookie 技术的目的。在用户自我控制方面,40 款 APP 表示用户可以拒绝使用 Cookie 技术,37 款在用户拒绝使用同时告知用户相关后果,即无法使用依赖 Cookie 的服务或需更改用户设置。

除信息收集种类外,运营商还需说明信息收集面向的群体。一般来说,移动健康 APP 主要向成年人提供服务。在缺乏监护人同意时,未成年人不得私自创建和使用账户。在涉及未成年人相关信息时,只会在法律允许和监护人明确同意后,才能收集、使用和披露,同时应删除未征得监护人同意的未成年人信息。调查结果发现,44 款 APP(占 42.31%)的隐私政策中明确标注了未成年人信息保护规定,明确表示当收集未成年人信息时,应征得未成年人本身或者监护人同意。其中有 9 款 APP 根据民事行为能力对儿童用户的年龄进行了详细界定:7 款 APP 将年龄低于 14 周岁视为未成年人,2 款将低于 16 周岁视为未成年人。另外,为保证未成年人信息保护的可操作性,"导医通"等 5 款 APP 在隐私政策中明确表示,必须提供监护人的书面同意,未成年人才可以注册使用 APP。

2.2.3 个人信息存储阶段

在用户的信息存储阶段,软件开发商和运营商应在隐私政策中对信息存储的地点、存储时限以及保护措施等做出详细说明。调查结果显示,104 款 APP 中有 33 款 APP 明确告知了存储地点。由于调查选取的移动健康 APP 均面向国内用户,一般承诺会将用户的个人相关信息保存在境内服务器上,不会在全球范围内转移。104 款 APP 中,有 16 款告知了存储期限,表示只在合理期限内存储用户的个人信息,当用户注销账户且超过后悔期后,会从系统删除个人信息或进行匿名化处理。比如,"叮当快药"明确表示会在用户注销 1 个月后删除或者匿名化处理个人信息。

在信息存储安全措施方面,61 款 APP(占58.65%)的隐私政策中包含了一项或多项信息安全存储保护措施。信息安全保护措施一般包括:①防止不当使用或未经授权的情况下访问、公开披露、使用、修改、损坏、丢失或泄漏个人信息;②通过加密技术、匿名化处理等防止个人信息遭到恶意攻击;③建立专门的安全部门、安全管理制度和数据安全管理流程;④尽力避免收集无关的个人信息,个人信息仅在合理期限内保留;⑤积极采取保护措施,谨慎向他人提供个人信息;⑥不定期更新并公开安全风险、个人信息安全影响评估报告等;⑦制定应急处理预案,并在发生用户信息安全事件时立即启动应急预案,努力阻止该等安全事件的影响和后果扩大。采取各安全存储保护措施的 APP 数量如

表4所示。对于个人信息的安全事件发生后的应急处置,有24款(占23.08%)APP给出了处置方案表示会及时告知用户相关信息,包括信息侵害事件的基本情况和可能的影响、平台已经采取或将要采取的处置措施、用户可自主防范和降低风险的建议、对用户的补救措施等。其中有20款(占19.23%)表示还会及时上报国家信息安全部门;13款(占12.50%)表示愿意承担用户隐私信息泄露的法律责任。

表4 104款APP隐私政策安全存储与保护设施情况

安全存储保护措施	APP数目(款)	占比(%)
防止您的个人信息遭到恶意攻击	55	52.88
个人积极采取保护措施	44	42.31
防止不当使用或未经授权的情况	40	38.46
个人信息安全事件应急处置	24	23.08
建立专门安全部门、管理制度及流程	20	19.23
避免收集无关信息,在合理期限内保留	19	18.27
更新并公开安全风险、评估报告等	8	7.69

注:一款抽样APP会采用一种或多种安全保护措施

2.2.4 个人信息使用阶段

在信息使用阶段,用户可能因为医患之间、患者之间的健康、诊疗咨询泄露自身的健康隐私信息。一方面,用户为获得个性化、高质量的医疗健康信息,可能会主动向医生披露个人的健康信息;另一方面,用户为在社交媒体上获得关注而通过话题、帖子、文章等形式发布其就医经历等个人健康信息,并在健康社区中与其他用户进行交流互动。皮尤研究中心调查结果显示,2012年美国约26%的网民阅读别人对健康或医疗问题的经验,约16%的用户查找与自身有相同健康问题的人[23]。在信息使用阶段,用户对自身信息拥有一定的支配权。一般包括访问、删除、更正个人信息,自主选择控制个性化推荐信息,改变授权同意范围或撤销授权,注销账号,等等。调查结果显示,44款APP(占42.31%)的隐私政策明确表示用户能够查询、更正或删除个人信息;33款APP(占31.73%)告知用户拥有注销账号的权利;另有24款APP(占23.08%)表示用户能够改变授权同意范围或撤销授权,其中23款告知了用户改变授权或撤销授权的流程或后果,详见表5。

《规范》规定,个人有权利拒绝和终止移动APP对个人信息的使用;但大部分APP(71款,占68.27%)并没有按照用户意愿完全终止对用户信息的使用,而是采取脱敏或去标识化处理后继续使用用户的个人信息。

表5 隐私政策用户自身权利与使用信息情况

用户自身权利	APP数目(款)	占比(%)
访问、更正或删除个人信息	44	42.31
注销账号	33	31.73
改变授权同意范围或撤销授权	24	23.08
响应上述请求	22	21.15
约束信息系统自动决策	18	17.31
停止运营告知	7	6.73
个人主体获取信息副本	6	5.77
申诉举报	6	5.77
自主选择控制个性化推荐信息	5	4.81
访问隐私政策	1	0.96
有关敏感信息的提醒	1	0.96

注:用户拥有一种或多种权利和信息支配权

2.2.5 个人信息共享阶段

部分服务提供方为了提高流量和用户黏度,会与第三方药品器械网站、健康咨询类网站或学术科研机构进行合作,开发其他附加服务。这些额外的服务增加了用户个人健康信息的泄漏风险。同时,由于个人健康信息拥有巨大的商业价值,可能会通过“信息二次交易市场”的灰色利益链条,被医生、患者及平台之外的第三方非法买卖或窃取。

《规范》规定,个人信息原则上不得转让和共享。个人信息控制者确需转让与共享时,应当充分重视此过程中信息泄露的风险。表6所示的调查结果显示,104款APP中有13款存在附属机构,9款APP会与其附属机构共享用户的个人信息;86款APP(占82.69%)会与第三方共享用户数据,主要包括用户自身授权、法律法规规定、与关联公司和合作伙伴共享、学术研究、处理与他人的纠纷或争议、帮助登录第三方和程序化广告推送以及用户需求健康建议时等9种情形。在是否共享Cookies方面,共有4款APP明确表示会与附属机构或第三方共享Cookies。

在信息披露的具体情形方面,39款APP表示会在用户知情同意下,公开披露个人信息;63款APP会在用户违法法律法规或者法律法规强制规定下,向社会披露用户个人信息;当用户存在违规和欺诈行为时,17款APP表示会在处罚公告中公开披露用户相关的信息。

在对特殊情况的处理上,75款APP(占72.12%)表示用户需要在同意披露个人信息的前提下才能获得某些特定服务。90款APP(占86.54%)表示会在法律要求下或在维护公众权益的情况下披露用户信息。此外,当出现用户自身授权、法律法规规定和符合与用户

签署的协议或者 APP 运营商出现业务转让、收购和合并等情形时,42 款 APP 表示个人信息库可以转让给第三方,其中 28 款 APP 表示接收转让方也会遵守当前隐私政策或者制定更严格的政策。

表 6　隐私政策个人信息共享、转让与披露情况

信息共享、转让和披露阶段指标			APP 数目(款)	占比(%)
信息共享	与第三方共享数据	用户自身授权	58	55.77
		法律法规规定	51	49.04
		与合作伙伴共享	42	40.38
		与关联公司共享	29	27.88
		学术研究	9	8.65
		处理与他人的纠纷或争议	8	7.69
		程序化广告推送	2	1.92
		需求健康帮助的建议	2	1.92
		帮助登录第三方	1	0.96
		总计	86	82.69
	存在附属机构		13	12.50
	与附属机构共享用户信息		9	8.65
	共享 Cookies		4	3.85
信息披露	违反法律规定或法律强制要求		63	60.58
	用户自身授权		39	37.50
	违规和欺诈行为进行处罚公告		17	16.35
特殊情形披露	法律要求或维护公众权益		90	86.54
	用户授权同意获取特定的服务		75	72.12
	信息转让	破产、合并、收购以及清算等	42	40.38
		用户自身授权	25	24.04
		符合签署的协议(如:交易)	25	24.04
		法律法规规定	8	7.69
		总计	42	40.38

注:一款抽样 APP 会存在一种或多种信息共享、转让和披露情形

2.2.6　信息咨询与反馈

当用户对隐私政策存在疑问时,可以通过 APP 提供的电话、邮箱、地址等方式联系运营商,因此,隐私政策中应明示信息咨询的途径和方式。调查结果显示,47 款 APP(占 45.2%)表示能够处理疑问和投诉,并提供联系渠道。"华医通"等 3 款 APP 还设立了个人信息保护专职部门或专员。但在投诉响应处理期限的承诺方面,仅有 19 款 APP 给出了期限,时间从 5 到 30 个工作日不等。"健康之路"等 9 款 APP 在隐私政策中提示用户认为自身合法权益受到侵犯时,可在有管辖权的法院提起诉讼。"轻松筹"和"叮当快药"还提供了其他的投诉或举报渠道,如网信、电信、公安、工商及民政等监管部门。

2.2.7　评价指标体系的构建及评价结果

为更全面地比较 104 款移动健康 APP 的隐私政策质量,本研究基于数据生命周期的视角,结合已有研究和《规范》内容构建了隐私政策综合评价体系。根据各指标选项之间的等级和对立关系,对各选项进行分数赋值,每个三级指标赋予相同的权重。当选项为"是"或"否"时,符合条件赋值为 1,不符合条件赋值为 0。当有多个选项时,每个选项赋予相同分值,满足一个选项给予相应赋值,例如指标 C11 有 3 个选项,满足一个得分为 1/3,满足两个得分为 2/3,三个都满足得分为 1 分,如表 7 所示。综合统计各 APP 满足条件的三级指标个数即为每个 APP 的测量结果,换算成百分制后,即为每个 APP 的最终得分。

通过对 104 款移动健康 APP 的隐私政策进行综合评价发现,移动健康 APP 在用户隐私保护政策方面整体表现欠佳,如图 1 所示,得分呈现非正态分布,以 100 分为满分计算得到平均分为 44.58 分,提示目前隐私政策的保护效果未达到良好状态(详见表 8)。得分在 0－60 分的移动健康 APP 有 77 个,占总数的 74.04%;得分在 61－80 分的有 14 个,占总数的 13.46%;得分在 80 分以上的有 13 个,占 12.50%。

表 7 移动健康 APP 的隐私政策综合评价体系

一级指标	二级指标	三级指标	选项	分值
A1 隐私政策属性	B1 隐私政策的属性	C1 隐私政策位置	1 = 手机端可查询、0 = 手机端不可查询	0、1
		C2 隐私文本长度(字数)	1 = 隐私文本长度大于等于所有文本的中位数、0 = 隐私文本长度小于中位数	0、1
	B2 隐私政策动态性	C3 最近更新时间	1 = 标注更新时间、0 = 未标注更新时间	0、1
A2 信息收集	B3 用户个人信息收集	C4 收集用户个人信息的种类	0 = 无说明、1 = 个人身份证明数据、2 = 通信通讯数据、3 = 个人健康生理信息等数据、4 = 个人财产信息、5 = 位置信息等数据、6 = 其他统计数据	0、1/6、1/6、1/6、1/6、1/6、1/6
	B4 未成年人信息收集	C5 是否规定未成年人信息保护	0 = 否、1 = 是	0、1
	B5 如何告知 Cookies	C6 是否说明使用 Cookies	0 = 否、1 = 是	0、1
		C7 Cookies 能否被禁用	0 = 否、1 = 是	0、1
		C8 是否说明了禁用 Cookies 的后果	0 = 否、1 = 是	0、1
A3 信息存储	B6 用户信息安全性	C9 是否有信息安全存储和保护措施	0 = 否、1 = 是	0、1
		C10 是否有安全事件处置措施	0 = 否、1 = 是	0、1
		C11 信息安全事件处置措施种类	0 = 无说明、1 = 及时告知、2 = 上报信息安全事件、3 = 承担法律责任	0、1/3、1/3、1/3
A4 信息使用	B7 用户信息自身访问	C12 个人信息能否查询	0 = 否、1 = 是	0、1
	B8 用户信息的使用	C13 个人信息能否处理如更正、删除等	0 = 否、1 = 是	0、1
		C14 是否有个人信息的使用目的和方式	0 = 否、1 = 是	0、1
		C15 使用个人信息时是否需告知用户、征得同意	0 = 否、1 = 不完全 *、2 = 完全	0、1/2、1
	B9 用户选择权	C16 使用个人信息时,个人是否有权利拒绝和终止	0 = 否、1 = 不完全 *、2 = 完全	0、1/2、1
		C17 用户能否退出网站定制服务	0 = 否、1 = 是	0、1
		C18 是否有用户行使选择权的后果	0 = 否、1 = 是	0、1
A5 信息共享	B10 与附属机构、第三方共享的说明	C19 是否说明与附属机构共享数据	0 = 否、1 = 是	0、1
		C20 是否说明与第三方共享数据	0 = 否、1 = 是	0、1
		C21 用户能否拒绝将数据给第三方共享	0 = 否、1 = 是	0、1
		C22 是否说明第三方使用 Cookies	0 = 否、1 = 是	0、1
		C23 是否出售数据	0 = 是、1 = 否	0、1
	B11 数据转让与披露的免责	C24 是否有特定情形下的信息披露	0 = 无说明、1 = 服务要求、2 = 法律要求、3 = 业务转让	0、1/3、1/3、1/3
A6 咨询与反馈	B12 用户的申诉权	C25 是否有用户隐私疑问的处理	0 = 否、1 = 是	0、1
		C26 是否有网站的联系方式	0 = 否、1 = 是	0、1
		C27 是否有对投诉的态度和应对措施	0 = 否、1 = 是	0、1

注:"*"表示能识别出个人身份的敏感信息需用户同意并授权,其余信息采取脱敏或去标识化处理后使用

表 8 APP 隐私文本分数描述统计值

统计量	最大值	最小值	平均值	标准差	中位数	四分位间距(Q75 – Q25)
分值	90.74	7.41	44.58	22.902	38.58	64.81 – 27.31

就指标体系评估得分来看,评分较低的三级指标包括隐私政策维度中的"更新时间"指标 21 分;数据存储维度中的"信息安全事件处置措施种类"指标 15 分;数据使用维度中的"是否有用户行使选择权的后果"指标 22 分;数据共享维度中的"是否说明与附属机构共享数据"和"是否说明第三方使用 Cookies",分别为 13 分和 7 分。

3 完善移动健康 APP 隐私政策的对策建议

随着国家标准《个人信息安全规范》(GB/T35273 –2017)的实施,对移动健康 APP 隐私政策的规范和监管工作更加严格。因此,还需要优化 APP 的隐私政策设计,促进移动健康 APP 隐私政策的规范制定,同时建立隐私政策质量的评价标准和监管机制,健全个人健康隐私信息的法律法规,以保障用户的安全、有效使用。

3.1 提高隐私政策文本的可见性和可读性

随着"互联网 + 医疗健康"发展,用户使用移动健

马骋宇，刘乾坤. 移动健康应用程序的隐私政策评价及实证研究[J]. 图书情报工作,2020,64(7):46－55.

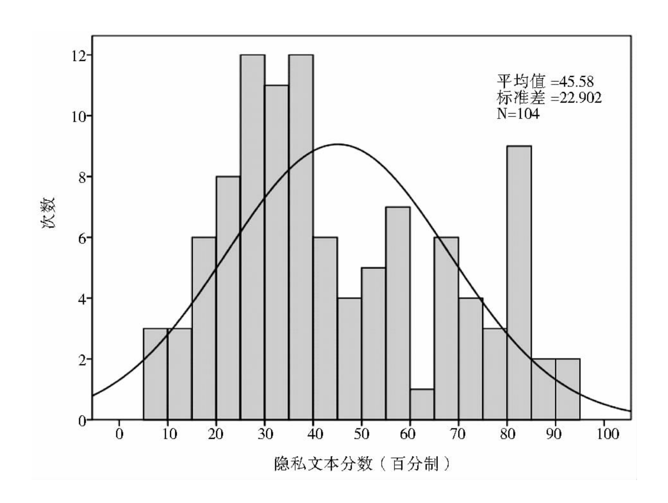


图 1　104 款移动健康 APP 的隐私政策综合评分分布

康 APP 的机会越来越多。但通过调查研究发现，目前移动健康 APP 的隐私保护效果还不理想，存在过度收集和滥用个人健康隐私信息的现象。因此，需要通过加强移动健康 APP 的隐私政策设计及使用规范来提升用户隐私保护水平。可见性和可读性是隐私政策重要的合规标准，是评价隐私政策完整性的重要内容[5]。在可见性方面，运营商需要在显著位置标注隐私政策条目，同时能够有效跳转到隐私政策文本。标题应包含“隐私”字眼，但不限于“隐私政策”“隐私声明”“隐私权保护”“隐私权指示”“个人隐私信息保护”等。在可读性方面，隐私政策应按照《规范》中的框架进行设计；隐私政策应尽可能规范、清晰，便于阅读，可以通过设置目录索引对内容进行提示，能够及时更新内容。

3.2　进一步优化移动健康 APP 的隐私保护政策

首先，隐私政策需根据服务内容明确界定所采集的个人健康信息的种类和用途。调查结果显示，多数移动健康 APP 的隐私政策对个人健康信息（包括身份信息和健康诊疗信息）进行了界定。但随着移动健康 APP 服务模式和服务内容的逐步创新，新的服务内容涉及到的个人健康信息应根据提供的个性化服务进行扩充和更新。如国外的一些医患社交 APP 将纳入保护的个人健康信息扩展到了患者与医生，或者患者与健康服务提供者之间的咨询交流和互动信息。此外，欧美一些国家也将可识别身份的死者信息纳入个人健康信息的主体保护范围之内[24]。

然后，应将个人健康信息纳入全生命周期的安全保护中，通过隐私政策进行完善和明确：

（1）在信息产生阶段，隐私政策中需要明确所遵守的法律法规，如欧美的移动健康 APP 会标注是在 HIPAA 或者 GDPR 框架约束下适用[25]。而我国移动健康 APP 没有明确标注。

（2）在信息收集阶段，应遵循目的明确、选择同意、最少够用等原则，避免个人信息的过度采集；详细说明信息收集的种类、目的和方式，并做好信息的安全风险评估。

（3）在信息存储环节，为确保个人信息的安全存储，需完善个人健康信息的保留期限，如英国 Babylon Health 公司的移动应用程序规定：全科医生记录在患者死亡后或患者永久离开该国后保留 10 年，产科记录需要保存到最后一个孩子出生的 25 年后[26]。

（4）在信息使用环节，运营商在使用用户信息前需提前告知，避免过度授权；收集老年人和未成年人信息时需要进行年龄限定，并有针对性地提供安全知识科普。美国食品药品监督管理局（Food and Drug Administration，FDA）规定一些移动健康 APP 需要每年向用户提供一份报告，报告内容包括收集和使用用户信息的种类，如果向第三方共享信息，还需要提供第三方机构名称和共享信息种类[27]。

（5）在信息共享和反馈阶段，用户拥有访问、更正、删除和注销个人账号的权利。运营商需要共享或转让用户个人信息时，需采取去标识或匿名化处理，并在隐私政策中进行说明。如果涉及跨国业务的 APP，还应公布其遵守的国际隐私政策框架，以保障在不同国家之间传递信息的安全。

（6）在信息反馈阶段，隐私政策需注明具体操作流程，并提供咨询和反馈的沟通渠道。

3.3　规范移动健康 APP 的隐私保护的评价和监管机制

用户隐私信息的保护不止是制定隐私条款，还需要落实条款中承诺的具体内容。但针对移动健康 APP 目前尚缺乏统一的评价标准和监管机制。相对于其他行业应用，移动健康 APP 面临着相对更高的信息安全风险。医疗服务存在信息不对称情况，医疗服务提供者及运营商可能在诊疗过程中收集了患者过多的隐私信息，其过程不容易被察觉。因此，必须遵循“包容谨慎、安全有序”的原则，加强移动健康 APP 的质量和数据安全监管，切实防范风险，在发展中保证安全，守住底线。针对健康隐私信息的特殊性，有关部门应构建互联网医疗健康及移动 APP 的隐私保护政策评价体系和监管机制：定期对隐私政策的规范性和可操作性做出评价，利用技术标准检测移动健康 APP 的安全性和稳定性，对不符合要求的 APP 进行下架处理；督促运营商落实企业主体责任，设立个人信息安全专职部

门和专员，以应对信息安全事件的发生；加强内部管理，定期审核内部工作人员的操作权限，注重离职保密协议的签订以及信息安全的培训与考核，防止工作人员因经济利益驱使、出于好奇心理等原因泄露用户医疗健康数据。

3.4 完善用户健康隐私信息保护的法律环境

个人健康信息的隐私安全保护，除了依赖隐私政策的制定和实施，还需要从法律层面来规范用户健康信息的使用，从而达到既能保证用户的合法权利，又能更好地促进"互联网 + 医疗健康"发展的目的。但是，相对于美国的《消费者隐私保护法案》和欧盟的《通用数据保护条例》，我国颁布的《规范》缺乏强制性和专业针对性，在个人健康隐私信息的保护方面指导性不足[6]。因此，首先需要从法律层面明确规定个人健康信息的内容，清晰界定在互联网及其移动 APP 上收集、使用、共享、管理、转让披露健康信息过程中所应保护的范围。其次，明确个人健康信息的归属权。用户在移动健康 APP 上分享个人健康信息，但很少主动管理自身信息。对于医疗机构、运营商对用户隐私信息的使用处置权限，需要进行清晰的界定。最后，由于用户与运营商之间存在信息不对称，在发生信息安全事件时，用户无法及时得知自身信息是否泄露及严重程度。因此，法律应明确运营商的取证义务，还应有明确的权利救济机制，确保当信息主体遭遇信息泄露及其带来的伤害时，能够获得一定的补偿或赔偿，保护在安全事件发生后用户的合法权益。

参考文献：

[1] 马晓伟. 加快互联网医疗创新融合发展 助力健康中国建设再上新台阶[J]. 时事报告(党委中心组学习)，2018(5)：43－55.
[2] 张秀兰. 网络隐私权保护研究[M]. 北京：北京图书馆出版社，2006：113－128.
[3] 王晰巍，相甍甍，张长亮，等. 新媒体环境下信息隐私国内外研究动态及发展趋势[J]. 图书情报工作，2017，61(15)：6－14.
[4] 何培育，马雅鑫，涂萌. Web 浏览器用户隐私安全政策问题与对策研究[J]. 图书馆，2019(2)：19－26.
[5] 中国消费者协会. 100 款 App 个人信息收集与隐私政策测评报告[EB/OL]. [2019－06－28]. http://www.cca.org.cn/jmxf/detail/28310.html.
[6] 何岚. 个人健康信息开发与保护的价值冲突及其治理[J]. 电子政务，2018(1)：92－99.
[7] SUNYAEV A, DEHLING T, TAYLOR P L, et al. Availability and quality of mobile health app privacy policies[J]. Journal of the American Medical Informatics Association, 2014, 22(1): e28－33.
[8] ZAPATA B C, NINIROLA A H, FERNANDEZ-ALEMAN J L, et al. Assessing the privacy policies in mobile personal health records [C]//IEEE. 2014 36th annual international conference of the IEEE engineering in medicine and biology society. Chicago: IL, 2014: 4956－4959.
[9] MARIAM B, ALI I, FERNANDEZ-ALEMAN J L, et al. Evaluating the privacy policies of mobile personal health records for pregnancy monitoring[J]. Journal of medical systems, 2018, 42(8): 1－14.
[10] SUNYAEV A, DEHLING T, TAYLOR P L, et al. Availability and quality of mobile health app privacy policies[J]. Journal of the American Medical Informatics Association, 2015, 22(4): 28－33.
[11] 冯嘉诚，郜独秀，陈洪淼. 基于用户隐私泄露预防的运动健康类 App 发展对策研究[J]. 吉林体育学院学报，2016，32(6)：63－69.
[12] 罗维娜，李澍，王晨希，等. 移动医疗网络安全监管策略研究[J]. 中国医疗设备，2017，32(6)：20－22，31.
[13] CROLL P R. Determining the privacy policy deficiencies of health ICT applications through semi-formal modelling[J]. International journal of medical informatics, 2011, 80(2): e32－38.
[14] ROWAN M, DEHINGER J. A Privacy policy comparison of health and fitness related mobile applications [J]. Procedia computer science, 2014, 37(9): 348－355.
[15] 朱颖. 我国移动 APP 隐私保护政策研究——基于 96 个移动应用 APP 的分析[J]. 暨南学报(哲学社会科学版)，2017，39(12)：107－114.
[16] 刘娇，白净. 中外移动 APP 用户隐私保护文本比较研究[J]. 汕头大学学报(人文社会科学版)，2017，33(3)：82－87.
[17] POWELL A C, SINGH P, TOROUS J. The complexity of mental health app privacy policies: a potential barrier to privacy[J]. JMIR mHealth and uHealth. 2018, 6(7): e158.
[18] PARKER L, HALTER V, KARLIYCHUK T, et al. How private is your mental health app data? an empirical study of mental health app privacy policies and practices[J]. International journal of law and psychiatry, 2019, 64(3): 198－204
[19] ROSENFELD L, TOROUS J, VAHIA I V. Data security and privacy in apps for dementia: an analysis of existing privacy policies [J]. The American journal of geriatric psychiatry, 2017, 25(8): 873－877.
[20] ROBILLARD J M, FENG T L, SPORN A B, et al. Availability, readability, and content of privacy policies and terms of agreements of mental health apps[J]. Internet interventions, 2019, 17(9): 1－8.
[21] KANTAR: 智能手机操作系统市场份额[EB/OL]. [2019－10－07]. https://www.kantarworldpanel.com/cn/smartphone-os-market-share/.
[22] 马文峰. 试析内容分析法在社科情报学中的应用[J]. 情报科学，2000(4)：346－349.
[23] SUSANNAH F. The social life of health information [EB/OL]. [2019－07－15]. http://www.pewresearch.org/fact-tank/2014/01/15/the-social-life-of-health-information/.

[24] 姜雯.国外个人健康信息基本要素介评及其启示[J].中国全科医学，2016，19(30):3652-3656.
[25] 李卓卓,马越,李明珍.数据生命周期视角中的个人隐私信息保护——对移动APP服务协议的内容分析[J].情报理论与实践,2016,39(12):63-68.
[26] Babylon privacy policy[EB/OL]. [2019-10-07]. https://www.babylonhealth.com/terms/privacy.
[27] Carbon health privacy policy[EB/OL]. [2019-10-07]. https://carbonhealth.com/privacy-policy.

作者贡献说明：
马骋宇：论文选题制定，研究框架构建，论文撰写；
刘乾坤：文献综述和资料收集，论文修改。

Research on the Privacy Policy's Evaluation and Empirical Study of Mobile Health Applications

Ma Chengyu　Liu Qiankun
Department of Health Management and Policy, School of Public Health,
Capital Medical University, Beijing 100069

Abstract: [**Purpose/significance**] To analyze the safety situation of privacy policy based on popular mobile health applications and propose to improve the privacy protection mechanism. [**Method/process**] 104 privacy policy texts of mobile health applications were selected as research objects through three rounds of screening. The content of the text was analyzed based on the content analysis method, and evaluated by a comprehensive evaluation system. [**Result/conclusion**] The overall evaluation score of mobile health apps' privacy policy is relative low, with the average score of 44.58 (100 full marks). Privacy policy needs to be improved in terms of content normatively and completeness. Some apps have the situation of excessive information collection and personal health privacy data abuse. The suggestions are proposed from 3 aspects, including optimizing the privacy policy design of apps, standardizing the privacy policy evaluation and supervision mechanism, and improving the legal environment for protecting users' health privacy information.

Keywords: privacy policy　mobile health　privacy protect　assurance mechanism